CLAIMS

What is claimed is:

1. A method for filtering packets, wherein a flow corresponds to a stream of packets for a particular communication session, comprising:

identifying a protocol used to transmit a packet;

identifying the flow to which the packet belongs;

determining whether a rules table exists for the protocol;

determining, if the rules table exists, whether a state table includes a matching flow entry corresponding to the flow;

determining, if the state table includes the matching flow entry, whether a state of the flow will transition from a current state indicated in the matching flow entry to a valid destination state indicated in a state-transition rule in the rules table; and

discarding the packet, if the state of the flow will not transition to the valid destination state.

2. The method of claim 1, wherein the protocol comprises a protocol whose operation is capable of being defined by a finite state machine.

3. The method of claim 2, wherein the protocol comprises one of the following: File Transfer Protocol, Telnet, Hypertext Transfer Protocol, H.323, Real Time Transport Protocol/Real Time Control Protocol and Secure Shell Protocol.

4. The method of claim 1, further comprising discarding the packet, if no rules table exists for the protocol.

5. The method of claim 1, further comprising transmitting the packet if no rules table exists for the protocol.

6. The method of claim 1, further comprising transmitting the packet if the flow will transition to the valid destination state.

7. The method of claim 1, further comprising:

determining whether the flow causes a skip count to be reached, wherein the skip count indicates a flow to examine after skipping a number of flows;

examining the flow, if the flow causes the skip count to be reached;

resetting the skip count, if the flow is examined;

skipping the flow, if the flow fails to cause the skip count to be reached; and

incrementing the skip count, if the flow is skipped.

8. The method of claim 7, further comprising:

determining that a number of actual flows fails to exceed a preset threshold of flows; and

examining flows based on the skip count, as a result of the number of actual flows failing to exceed the preset threshold.

9. The method of claim 7, further comprising:

determining that a number of actual flows exceeds a preset threshold of flows;

determining a number of preset steps by which the number of actual flows exceeds the preset threshold;

multiplying the number of preset steps by a preset skip-count modifier; and

changing the skip count to a different skip count equal to the product of the preset number of steps and the preset skip-count modifier.

10. The method of claim 1, wherein determining whether the state table includes the matching flow entry comprises:

performing a hashing function based, at least in part, on values in the packet;

determining whether a flow entry matches a result of the hashing function;

determining, if the flow entry matches the result, whether the packet values hashed to generate the result match values used to generate the flow entry; and

determining, if the packet values match the values used to generate the flow entry, that the flow entry is the matching flow entry.

11. The method of claim 10, further comprising:

performing one or more additional hashing functions according to a number related to a skip count, if no flow entry matches the result of the hashing function, wherein the skip count indicates a flow to examine after skipping a number of flows; and

performing the one or more additional hashing functions according to the number related to the skip count, if the flow entry matches the result of the hashing function, but the packet values fail to match the values used to generate the flow entry.

12. The method of claim 11, wherein performing the one or more additional hashing functions according to the number related to the skip count comprises:

performing a preset minimum number of additional hashing functions, if the skip count comprises a first value;

performing an increased number of additional hashing functions, if the skip count is increased, wherein the increased number of additional hashing functions is greater than the preset minimum number of additional hashing functions, but less than a preset maximum number of additional hashing functions; and

performing the preset maximum number of additional hashing functions, when the increased number of additional hashing functions reaches the preset maximum number of additional hashing functions.

13. The method of claim 10, further comprising:

identifying, if the state table fails to include the matching flow entry, a set of one or more state-transition rules having an indication to create an additional flow entry;

determining whether the packet includes a transition pattern indicated in a state-transition rule in the set, wherein the transition pattern indicates that the additional flow entry is to be created;

creating the additional flow entry, if the packet includes the transition pattern; and

discarding the packet, if the packet fails to include the transition pattern.

14. The method of claim 1, wherein determining whether the state of the flow will transition to the valid destination state comprises:

performing an operation using the current state and combined source states indicated in a state-transition rule;

determining whether the current state matches a result of the operation;

determining, if the current state matches the result of the operation, that the combined source states include the current state;

determining, as a result of the combined source states including the current state, whether the packet includes a transition pattern indicated in the state-transition rule; and

determining, if the packet includes the transition pattern, that the state of the flow will transition from the current state to the valid destination state in the state-transition rule in the set.

15. The method of claim 14, wherein the operation comprises an AND operation.

16. The method of claim 14, further comprising:

identifying in the state-transition rule, if the state of the flow will transition to the valid destination state, a source state-destination state pair that includes the current state; and

replacing the current state with the destination state indicated in the source state-destination state pair.

17. The method of claim 16, further comprising:

determining whether the source state-destination state pair includes an evict indication; and

evicting the matching flow entry, if the source state-destination state pair includes the evict indication.

18. The method of claim 14, further comprising

discarding the packet, if the packet fails to include the transition pattern included in a plurality of state-transition rules whose combined source states include the current state.

19. The method of claim 1, wherein discarding the packet comprises:

determining whether the packet causes a predetermined number of packets associated with invalid transitions to be reached; and

discarding the packet, if the packet causes the predetermined number to be reached.

20. An apparatus comprising:

a classifier, to identify a protocol used to transmit a packet and identify a stream of packets to which the packet belongs, wherein the stream of packets comprises a flow;

one or more rules tables that include one or more state-transition rules;

one or more state tables for the protocol that include one or more flow entries and values used to generate the flow entries; and

a rules engine, to determine whether a rules table exists for the protocol, determine, if the rules table exists, whether the state table includes a matching flow entry corresponding to the flow, determine, if the state table includes the matching flow entry, whether the flow will transition from a current state to a valid destination state indicated in a state-transition rule, and discard the packet, if the flow will not transition to the valid destination state.

21. The apparatus of claim 20, wherein the rules engine determines whether the state table includes the matching flow entry by performing a hashing function based, at least in part, on values in the packet, determining whether a flow entry matches a result of the hashing function, determining, if the flow entry matches the result, whether the packet values hashed to generate the result match values used to generate the flow entry, and determining, if the packet values match the values used to generate the flow entry, that the flow entry is the matching flow entry.

22. The apparatus of claim 20, wherein the rules engine determines whether the state of the flow will transition to the valid destination state by performing an operation using the current state and combined source states indicated in a state-transition rule, determining whether the current state matches a result of the operation, determining, if the current state matches the result of the operation, that the combined source states

include the current state, determining, as a result of the combined source states including the current state, whether the packet includes a transition pattern indicated in the state-transition rule, and determining, if the packet includes the transition pattern, that the state of the flow will transition from the current state to the valid destination state in the state-transition rule in the set.

23. An article of manufacture comprising:

a machine-accessible medium including thereon sequences of instructions that, when executed, cause an electronic system to:

identify a protocol used to transmit a packet;

identify the flow to which the packet belongs;

determine whether a rules table exists for the protocol;

determine, if the rules table exists, whether a state table includes a matching flow entry corresponding to the flow;

determine, if the state table includes the matching flow entry, whether a state of the flow will transition from a current state indicated in the matching flow entry to a valid destination state indicated in a state-transition rule in the rules table; and

discard the packet, if the state of the flow will not transition to the valid destination state.

24. The article of manufacture of claim 23, wherein the machine-accessible medium further comprises sequences of instructions that, when executed, cause the electronic system to:

determine whether the flow causes a skip count to be reached, wherein the skip count indicates a flow to examine after skipping a number of flows;

examine the flow, if the flow causes the skip count to be reached;

reset the skip count, if the flow is examined;

skip the flow, if the flow fails to cause the skip count to be reached; and

increment the skip count, if the flow is skipped.

25. The article of manufacture of claim 24, wherein the machine-accessible medium further comprises sequences of instructions that, when executed, cause the electronic system to:

determine that a number of actual flows fails to exceed a preset threshold of flows; and

examine flows based on the skip count, as a result of the number of actual flows failing to exceed the preset threshold.

26. The article of manufacture of claim 24, wherein the machine-accessible medium further comprises sequences of instructions that, when executed, cause the electronic system to:

determining that a number of actual flows exceeds a preset threshold of flows;

determine a number of preset steps by which the number of actual flows exceeds the preset threshold;

multiply the number of preset steps by a preset skip-count modifier; and

change the skip count to a different skip count equal to the product of the preset number of steps and the preset skip-count modifier.

27. The article of manufacture of claim 23, wherein the sequences of instructions that, when executed, cause the electronic system to determine whether the state table includes the matching flow entry comprise sequences of instructions that, when executed, cause the electronic system to:

perform a hashing function based, at least in part, on values in the packet;

determine whether a flow entry matches a result of the hashing function;

determine, if the flow entry matches the result, whether the packet values hashed to generate the result match values used to generate the flow entry; and

determine, if the packet values match the values used to generate the flow entry, that the flow entry is the matching flow entry.

28. The article of manufacture of claim 27, wherein the machine-accessible medium further comprises sequences of instructions that, when executed, cause the electronic system to:

identify, if the state table fails to include the matching flow entry, a set of one or more state-transition rules having an indication to create an additional flow entry;

determine whether the packet includes a transition pattern indicated in a state-transition rule in the set, wherein the transition pattern indicates that the additional flow entry is to be created;

create the additional flow entry, if the packet includes the transition pattern; and

discard the packet, if the packet fails to include the transition pattern.

29. The article of manufacture of claim 23, wherein the sequences of instructions that, when executed, cause the electronic system to determine whether the state of the flow will transition to the valid destination state comprise sequences of instructions that, when executed, cause the electronic system to:

perform an AND operation using the current state and combined source states indicated in a state-transition rule;

determine whether the current state matches a result of the operation;

determine, if the current state matches the result of the operation, that the combined source states include the current state;

determine, as a result of the combined source states including the current state, whether the packet includes a transition pattern indicated in the state-transition rule; and

determine, if the packet includes the transition pattern, that the state of the flow will transition from the current state to the valid destination state in the state-transition rule in the set.

30. A system comprising:

a processor;

a network interface coupled with the processor; and

an article of manufacture comprising a machine-accessible medium including thereon sequences of instructions that, when executed, cause an electronic system to:

identify a protocol used to transmit a packet;

identify the flow to which the packet belongs;

determine whether a rules table exists for the protocol;

determine, if the rules table exists, whether a state table includes a matching flow entry corresponding to the flow;

determine, if the state table includes the matching flow entry, whether a state of the flow will transition from a current state indicated in the matching flow entry to a valid destination state indicated in a state-transition rule in the rules table; and

discard the packet, if the state of the flow will not transition to the valid destination state.

31. The system of claim 30, wherein the sequences of instructions that, when executed, cause the electronic system to determine whether the state table includes the matching flow entry comprise sequences of instructions that, when executed, cause the electronic system to:

perform a hashing function based, at least in part, on values in the packet;

determine whether a flow entry matches a result of the hashing function;

determine, if the flow entry matches the result, whether the packet values hashed to generate the result match values used to generate the flow entry; and

determine, if the packet values match the values used to generate the flow entry, that the flow entry is the matching flow entry.

32. The system of claim 30, wherein the machine-accessible medium further comprises sequences of instructions that, when executed, cause the electronic system to:

identify, if the state table fails to include the matching flow entry, a set of one or more state-transition rules having an indication to create an additional flow entry;

determine whether the packet includes a transition pattern indicated in a state-transition rule in the set, wherein the transition pattern indicates that the additional flow entry is to be created;

create the additional flow entry, if the packet includes the transition pattern; and

discard the packet, if the packet fails to include the transition pattern.

33. The system of claim 30, wherein the sequences of instructions that, when executed, cause the electronic system to determine whether the state of the flow will transition to the valid destination state comprise sequences of instructions that, when executed, cause the electronic system to:

perform an AND operation using the current state and combined source states indicated in a state-transition rule;

determine whether the current state matches a result of the operation;

determine, if the current state matches the result of the operation, that the combined source states include the current state;

determine, as a result of the combined source states including the current state, whether the packet includes a transition pattern indicated in the state-transition rule; and

determine, if the packet includes the transition pattern, that the state of the flow will transition from the current state to the valid destination state in the state-transition rule in the set.